What is claimed is:

1. An apparatus for providing verification of a security status of an on-line service, comprising:

a database that stores a profile of devices and services comprising the on-line service and a corresponding indication of their vulnerability; and

a verification engine that provides verification to visitors of the on-line service via a network by displaying an indication of the security status of the on-line service to the visitor in accordance with the stored profile,

wherein the visual appearance of the indication is changed in accordance with a level of security computed for the on-line service.

2. An apparatus according to claim 1, further comprising a scanning engine that detects the devices and services comprising the on-line service.

3. An apparatus according to claim 2, wherein the scanning engine further performs a comparison between vulnerability fingerprints and the devices and services to obtain the corresponding vulnerability indications.

4. An apparatus according to claim 1, wherein the apparatus is remote from the on-line service on the network.

5. An apparatus according to claim 4, wherein the apparatus is remote from the on-line service on the network.

6. An apparatus according to claim 1, wherein the displayed indication is made in response to the visitor clicking a bug displayed by the on-line service.

7. An apparatus according to claim 3, further comprising an alert engine that sends alerts to the on-line service in accordance with the comparison performed by the scanning engine.

8. An apparatus according to claim 7, wherein the alert engine further determines whether new vulnerabilities potentially affect the on-line service.

9. An apparatus according to claim 8, wherein the alert engine is operative to further determine whether new vulnerabilities potentially affect the on-line service based on information in the stored profile and newly received vulnerability information without requiring a new scan by the scanning engine to detect devices and services comprising the on-line service.

10. An apparatus according to claim 1, wherein the verification engine further receives requests for registration of new on-line services, the verification engine registering the new on-line services in accordance with a determination that a bug exists at a pre-defined URL.

11. An apparatus according to claim 1, wherein the on-line service is a website.

12. An apparatus according to claim 10, wherein the on-line service is a website.

13. An apparatus according to claim 1, wherein the network is the Internet.

14. An apparatus for providing verification of a security status of one or more on-line services, comprising:

a database that stores respective profiles of devices and services comprising the on-line services and corresponding indications of their vulnerability; and

a security website that receives requests for verification from actual or potential visitors of a selected one of the on-line services via a network and provides a graphical indication of the security status of the selected on-line service to the visitor in accordance with the stored profile,

wherein the visual appearance of the graphical indication is changed in accordance with a level of security computed for the selected one of the on-line services.

15. An apparatus according to claim 14, wherein the graphical indication is a security meter.

16. An apparatus according to claim 14, wherein the security website is further operative to provide graphical indicators of the security status of a plurality of the on-line services in accordance with the stored profiles and requests by the visitors.

17. An apparatus according to claim 14, further comprising a scanning engine that detects the devices and services comprising the on-line services.

18. An apparatus according to claim 17, wherein the scanning engine further performs a comparison between vulnerability fingerprints and the devices and services to obtain the corresponding vulnerability indications.

19. An apparatus according to claim 14, wherein the apparatus is remote from each of the on-line services on the network.

20. An apparatus according to claim 18, wherein the apparatus is remote from each of the on-line services on the network.

21. A method for providing verification of a security status of an on-line service, comprising:

detecting devices and services comprising the on-line service;

comparing the detected devices and services against vulnerability fingerprints;

receiving requests for verification from visitors of the on-line service via a network;

providing an indication of the security status of the on-line service to the visitor in accordance with a result of the comparing step; and

changing the visual appearance of the indication is changed in accordance with a level of security computed for the on-line service..

22. A method according to claim 21, wherein the comparing step includes scanning the on-line service from a remote address on the network.

23. A method according to claim 21, further comprising allowing the visitor to make the requests by clicking a bug displayed by the on-line service.

24. A method according to claim 21, further comprising sending alerts to the on-line service in accordance with the comparison performed by the scanning engine.

25. A method according to claim 24, wherein the alerting step includes determining whether new vulnerabilities potentially affect the on-line service.

26. A method according to claim 21, further comprising:

receiving a request for registration of a new on-line service;

determining whether a bug exists at a pre-defined URL in the request; and

registering the new on-line services in accordance with the determination that the bug exists at the pre-defined URL.